

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Ben-Chuan Du,) Group: Not yet assigned
) et al.
)
Serial No.: Not yet assigned)
) Examiner: Not yet assigned
Filed: Concurrently herewith)
) Our Ref: B-5166 621102-3
For: "DEVICE AND METHOD FOR)
SECURING INFORMATION ASSOCIATED) WITH A SUBSCRIBER IN A
COMMUNICATION APPARATUS") Date: July 10, 2003

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

[X] Applicants hereby make a right of priority claim under 35 U.S.C. 119 for the benefit of the filing date(s) of the following corresponding foreign application(s):

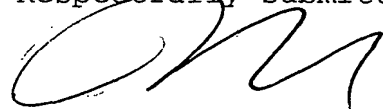
| <u>COUNTRY</u> | <u>FILING DATE</u> | <u>SERIAL NUMBER</u> |
|----------------|--------------------|----------------------|
| Taiwan, R.O.C. | 10 July 2002 | 91115362 |

[] A certified copy of each of the above-noted patent applications was filed with the Parent Application No. _____.

[X] To support applicant's claim, a certified copy of the above-identified foreign patent application is enclosed herewith.

[] The priority document will be forwarded to the Patent Office when required or prior to issuance.

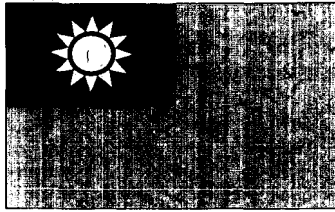
Respectfully submitted,



Richard P. Berg
Attorney for Applicant
Reg. No. 28,145

LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
Telephone: (323) 934-2300

EV 25733007545



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this
office of the application as originally filed which is identified hereunder:

申請日：西元 2002 年 07 月 10 日
Application Date

申請案號：091115362
Application No.

申請人：明基電通股份有限公司
Applicant(s)

局長
Director General

陳明邦

發文日期：西元 2002 年 8 月 28 日
Issue Date

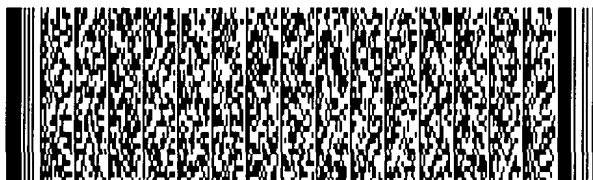
發文字號：
Serial No. 09111016557

| | | | |
|-------|-----------|-----|----------|
| 申請日期： | 91. 7. 10 | 案號： | 91115362 |
| 類別： | | | |

(以上各欄由本局填註)

發明專利說明書

| | | |
|------------|---------------------|--|
| 一、 發明名稱 | 中 文 | 通訊設備中用以保全用戶資訊之裝置及方法 |
| | 英 文 | DEVICE AND METHOD FOR SECURING INFORMATION ASSOCIATED WITH A SUBSCRIBER IN A COMMUNICATION APPARATUS |
| 二、 發明人 | 姓 名 (中文) | 1. 杜本權 2. 范振煌 |
| | 姓 名 (英文) | 1. Ben-Chuan Du 2. Chen-Huang Fan |
| | 國 籍 | 1. 中華民國 2. 中華民國 |
| | 住、居所 | 1. 台北縣新店市三民路75巷9弄12號2樓 2. 苗栗縣頭份鎮尖山里尖豐路52號 |
| 三、 申請人 | 姓 名 (名稱) (中文) | 1. 明基電通股份有限公司 |
| | 姓 名 (名稱) (英文) | 1. Benq Corporation |
| | 國 籍 | 1. 中華民國 |
| | 住、居所 (事務所) | 1. 桃園縣龜山鄉山鶯路157號 |
| | 代表人 姓 名 (中文) | 1. 李焜耀 |
| | 代表人 姓 名 (英文) | 1. Kuen-Yao Lee |



四、中文發明摘要 (發明之名稱：通訊設備中用以保全用戶資訊之裝置及方法)

本發明係提供一種用於一通訊設備內之裝置，該裝置係用以保全一用戶之一資訊。該通訊設備係包含一密鑰產生模組。根據本發明之裝置係包含一儲存模組、一密鑰取得模組、一加密模組以及一解密模組。該用戶之資訊係儲存於該儲存模組內。該密鑰取得模組係用以傳送一輸入資料至一密鑰產生模組，並且隨後接收由該密鑰產生模組回應該輸入資料所產生之一密鑰。該加密模組係用以經由該密鑰取得模組擷取該密鑰，並且從該儲存模組擷取該用戶之資訊，並且隨後使用該密鑰對該用戶之資訊加密，進而產生一加密資訊。於產生該加密資訊之後，該加密資訊係儲存於該儲存模組內，並且置換儲存於該儲存模組內該用戶之資訊。當該用戶之資訊需要被使用時，該解密模組係

英文發明摘要 (發明之名稱：DEVICE AND METHOD FOR SECURING INFORMATION ASSOCIATED WITH A SUBSCRIBER IN A COMMUNICATION APPARATUS)

The invention is to provide a device, used in a communication apparatus including a cipher key generating module, for securing an information associated with a subscriber. The device according to the invention includes a storage module, a cipher key acquiring module, an encrypting module and a decrypting module. The information associated with the subscriber is stored in the storage module. The cipher key acquiring module functions transmitting an input to the cipher key



四、中文發明摘要 (發明之名稱：通訊設備中用以保全用戶資訊之裝置及方法)

用以經由該密鑰取得模組擷取該密鑰，並且從該儲存模組擷取該加密資訊，並且隨後使用該密鑰對該加密資訊解密，進而恢復該用戶之資訊。其中，當該解密模組經由該密鑰取得模組擷取該密鑰時，該密鑰取得模組則再次傳送該輸入資料至該密鑰產生模組，並且隨後接收由該密鑰產生模組回應該輸入資料再次產生之該密鑰。藉此，達到該用戶之資訊的保全。

英文發明摘要 (發明之名稱：DEVICE AND METHOD FOR SECURING INFORMATION ASSOCIATED WITH A SUBSCRIBER IN A COMMUNICATION APPARATUS)

generating module, and then receiving a cipher key generated by the cipher key generating module in response to the input. The encrypting module functions retrieving the cipher key through the cipher key acquiring module, retrieving the information associated the subscriber from the storage module, and encrypting the information associated with the subscriber using the cipher key to generate an encrypted information. After generated, the encrypted information is stored into



四、中文發明摘要 (發明之名稱：通訊設備中用以保全用戶資訊之裝置及方法)

英文發明摘要 (發明之名稱：DEVICE AND METHOD FOR SECURING INFORMATION ASSOCIATED WITH A SUBSCRIBER IN A COMMUNICATION APPARATUS)

the storage module and replaces the information associated with the subscriber stored in the storage module. When the information associated with the subscriber needs to be used, the decrypting module functions retrieving the cipher key through the cipher key acquiring module, retrieving the encrypted information from the storage module, and decrypting the encrypted information using the cipher key to recover the information associated with the subscriber. When



四、中文發明摘要 (發明之名稱：通訊設備中用以保全用戶資訊之裝置及方法)

英文發明摘要 (發明之名稱：DEVICE AND METHOD FOR SECURING INFORMATION ASSOCIATED WITH A SUBSCRIBER IN A COMMUNICATION APPARATUS)

the decrypting module retrieves the cipher key through the cipher key acquiring module, the cipher key acquiring module transmits the input once more to the cipher key generating module, and then receives the cipher key generated once more by the cipher key generating module in response to the input. Thereby, the security of the information associated with the subscriber is achieved.



本案已向

國(地區)申請專利

申請日期

案號

主張優先權

無

有關微生物已寄存於

寄存日期

寄存號碼

無

五、發明說明 (1)

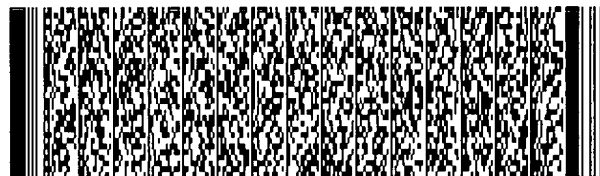
發明領域

本發明係提供一種用於通訊設備內之裝置，例如，家用電話、行動電話 (Mobile phone)、個人數位助理 (PDA)，以及其他行動通訊裝置等。根據本發明之裝置係用以保全一用戶之資訊，並且特別地該通訊設備包含一密鑰產生模組 (Cipher key generating module)，例如，插入行動電話內之用戶資訊模組卡 (Subscriber Information Module card, SIM card)，藉由利用該密鑰產生模組所產生之密鑰，進而對該用戶之資訊作加密、解密處理。藉此，達到該用戶之資訊的保全 (Security)。

發明背景

現行通訊設備，例如，行動電話、個人數位助理，以及其他行動通訊裝置等，大多已具備儲存資訊的功能，用以儲存例如通訊錄、行事曆…等關於用戶私密性的資訊。為防止未經用戶同意的第三人使用屬於該用戶之通訊設備，進而竊取該通訊設備中關於該用戶之私密資料，通訊設備通常需具備對該用戶之資訊保全的功能。

以現行的行動電話為例，皆需插入用戶資訊模組卡才可啟動通訊功能。用戶資訊模組卡本身具備產生密鑰的功能，由於現行內建於用戶資訊模組卡內，用以產生密鑰之演算邏輯，例如，混雜基礎訊息認證碼 (Hash-based Message Authentication Code, HMAC) 演算邏輯、GSM-A3 演算邏輯、GSM-A8 演算邏輯等，幾乎無法被破解。因此，



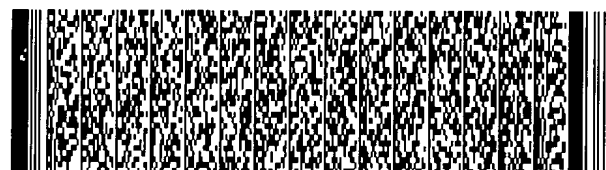
五、發明說明 (2)

用戶資訊模組卡咸被認同具有高度的保全設計。現行的行動電話可以藉由兩種方法達到保全用戶資訊之目的：其一是用戶自行選擇並輸入密碼，進而鎖住用戶資訊模組卡；其二是利用密碼鎖住行動電話。

上述第一種習知藉由用戶自行選擇並輸入密碼，進而鎖住用戶資訊模組卡的方法，是利用用戶資訊模組卡本身具有高度保全之設計，但卻僅能保全儲存於用戶資訊模組卡片內之資料，對於不儲存於用戶資訊模組卡內之資料，亦即儲存於行動電話內之資訊，則無保全的作用。也就是說，例如當行動電話遺失時，未經用戶同意之第三人只要換插入另一片用戶資訊模組卡至行動電話內，即能使用該支行動電話，進而竊取儲存於該支行動電話內之資訊。

上述第二種習知利用密碼鎖住行動電話的方法，讓拾取或竊取到行動電話的第三人在即便換插入另一片用戶資訊模組卡的情況下，亦無法使用該支行動電話。藉此，可以彌補上述第一種習知方法之缺點。然而，若該支行動電話需供多人使用時，則需另外設計一套系統來分別區分、辨識不同使用者的專屬密碼，如此的設計太複雜，且不利於產品成本之降低。

除此之外，上述第二種習知利用密碼鎖住行動電話的方法，其保全性的高低，牽涉到該密碼相關的電路設計。一般而言，現行行動電話等通訊設備本身關於輸入密碼的電路設計，仍留有極大的機會讓有心人士有破解密碼之餘裕。甚至，現行行動電話等通訊設備本身的設計，讓有心



五、發明說明 (3)

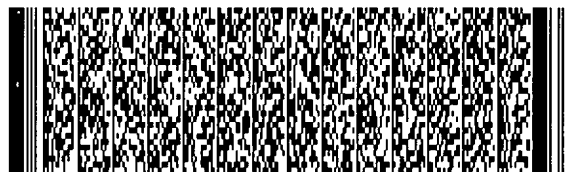
人士可以直接偵測其內部電話，直接竊取到用戶之資訊。

發明概述

關於現行的通訊設備，仍有無法對於用戶之資訊做到妥善的保全。因此，本發明之一目的即提供一種用於或執行於一通訊設備內之資訊保全裝置及方法，該資訊保全裝置及方法係用以保全該通訊設備之用戶的資訊。

此外，本發明之另一目的係提供一種用於或執行於一通訊設備內之資訊保全裝置及方法，該裝置及方法係利用該通訊設備原具有的密鑰產生功能所產生之密鑰，進而對該用戶之資訊作加密、解密處理。藉此，在不增添繁雜功能及不增加大幅成本下，達到該用戶之資訊的保全。

根據本發明第一較佳具體實施例之資訊保全裝置，係用於一通訊設備中，用以保全該通訊設備之用戶的資訊。該通訊設備並且包含一密鑰產生模組，用以產生密鑰。根據本發明之第一較佳具體實施例之資訊保全裝置包含一儲存模組、一密鑰取得模組、一加密模組以及一解密模組。該用戶之資訊係儲存於該儲存模組內。該密鑰取得模組係用以傳送一輸入資料至該密鑰產生模組，並且隨後接收由該密鑰產生模組回應該輸入資料所產生之一密鑰。該加密模組係用以經由該密鑰取得模組擷取該密鑰，並且從該儲存模組中擷取該用戶之資訊，並且隨後使用該密鑰對該用戶之資訊加密，進而產生一加密資訊。於產生加密資訊之後，該加密資訊係儲存於該儲存模組內並且置換儲存於該



五、發明說明 (4)

儲存模組內之用戶的資訊。當該用戶之資訊需要被使用時，該解密模組即經由該密鑰取得模組擷取該密鑰，並且從該儲存模組中擷取該加密資訊，並且隨後使用該密鑰對加密資訊解密，進而恢復該用戶之資訊。其中，當該解密模組經由該密鑰取得模組擷取該密鑰時，該密鑰取得模組係再次傳送該輸入資料至該密鑰產生模組，並且隨後接收由該密鑰產生模組回應該輸入資料而再次產生之密鑰。

關於本發明之優點與精神可以藉由以下的發明詳述及所附圖式得到進一步的瞭解。

發明之詳細說明

本發明之目的旨在提供一種供一通訊設備使用之資訊保全裝置，藉以對儲存於該通訊設備內之用戶的資訊做到妥善的保全。以下將詳述本發明之較佳具體實施例，藉以充分解說本發明之特徵、精神、優點以及應用上的簡便性。

請參考圖一，圖一係為根據本發明之第一較佳具體實施例之資訊保全裝置 10 的架構之示意圖。該資訊保全裝置 10 係用於一通訊設備 1 內，用以保全該通訊設備 1 之一用戶的資訊。該通訊設備 1 並且包含一密鑰產生模組 (Cipher key generating module) 12，該密鑰產生模組 12 係用以產生一密鑰 (Cipher key)。

該資訊保全裝置 10 係包含一儲存模組 102、一密鑰取得模組 (Cipher key acquiring module) 104、一加密模組



五、發明說明 (5)

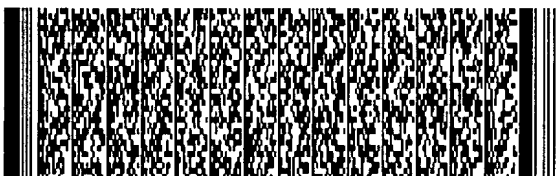
(Encrypting module)106以及一解密模組 (Decrypting module)108。關於該儲存模組 102，該用戶之資訊係儲存於該儲存模組 102內。該密鑰取得模組 104係用以傳送一輸入資料至該密鑰產生模組 12，此輸入資料可以是預存於該通訊設備 1內之一硬體序號，例如是通訊設備中手機的國際行動設備識別碼 (International Mobile Equipment Identity, IMEI)。該密鑰產生模組 12於接收到該輸入資料後，會回應該輸入資料，並且產生一密鑰。隨後，該密鑰取得模組 104接收由該密鑰產生模組 12回應該輸入資料所產生之密鑰。

於一具體實施例中，該密鑰產生模組 12係具有一預定演算邏輯，例如，圖一中所示的預定演算邏輯 122。該輸入資料係被代入該演算邏輯 122中，經過演算進而產生該密鑰。

於一具體實施例中，該密鑰產生模組 12係為一用戶資訊模組卡 (SIM card)。該預定演算邏輯係可為一 HMAC演算邏輯、一 GSM-A3演算邏輯或一 GSM-A8演算邏輯...等。

另外，產生密鑰的方法也可以不經由演算邏輯 122，而密鑰產生模組 12內預先存有一使用者代號，例如用戶資訊模組卡中的行動用戶識別碼 (International Mobile Subscriber Identity, IMSI)，該密鑰產生模組 12係回應該輸入資料進而輸出該使用者代號做為該密鑰之用。

該加密模組 106係用以經由該密鑰取得模組 104擷取該密鑰，並且從該儲存模組 102擷取該用戶之資訊。隨後，



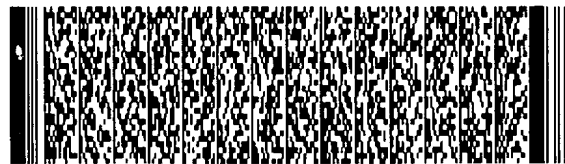
五、發明說明 (6)

該加密模組 106 使用該密鑰對該用戶之資訊加密，進而產生一加密資訊。需說明的是，於產生該加密資訊之後，該加密資訊係儲存於該儲存模組 102 內，並且置換儲存於該儲存模組 102 內之用戶的資訊。於實際應用中，如圖一所示，該加密模組 106 係由來自該通訊設備 1 之一驅動訊號所驅動，進而對該用戶之資訊加密。

進一步，當該用戶之資訊需要被使用時，該解密模組 108 係用以經由該密鑰取得模組 104 擷取該密鑰，並且從該儲存模組 102 擷取該加密資訊。隨後，該解密模組 108 使用該密鑰對該加密資訊解密，進而恢復該用戶之資訊。需說明的是，當該解密模組 108 經由該密鑰取得模組 104 擷取該密鑰時，該密鑰取得模組 104 係再次傳送該輸入資料至該密鑰產生模組 12，並且隨後接收由該密鑰產生模組 12 回應該輸入資料而再次產生之密鑰。於實際應用中，如圖一所示，該解密模組 108 係由來自該通訊設備 1 之一驅動訊號所驅動，進而對該加密資訊解密。

於實際應用中，該加密模組 106 以及該解密模組 108 係可以整合成一個模組。

由以上對第一較佳具體實施例的詳述，可清楚的瞭解對經過加密處理的用戶之資訊解密，需要再次取得密鑰。然而，該通訊設備 1 以及該資訊保全裝置 10 並不儲存密鑰。每次欲取得密鑰，必須使用到該密鑰產生模組 12，例如 SIM 卡。因此，當該通訊設備 1 遺失或是遭竊時，未經用戶同意之第三人若要對加密過的用戶之資訊解密，必須先



五、發明說明 (7)

破解原有的密鑰產生模組 12(例如, SIM卡)。一般而言, 密鑰產生模組 12 本身即具有高度的保全設計, 因此, 根據本發明之資訊保全裝置 10 對於用戶之資訊亦可做到充分的保全。並且, 根據本發明之資訊保全裝置 10 的設計簡單, 製造成本低廉。明顯地, 應用根據本發明之資訊保全裝置 10, 可在不增添該通訊設備 1 繁雜功能及不增加大幅成本下, 即達到該用戶之資訊的保全。

此外, 該通訊設備 1 係供多人使用時, 可以藉由每個人配屬專屬的密鑰產生模組 12(例如, SIM卡), 來達到每個人使用該通訊設備 1 時, 僅能對自己儲存於該通訊設備 1 內的資訊解密, 而無法破解其他人儲存於該通訊設備 1 內的資訊。藉此, 應用根據本發明之資訊保全裝置 10, 可在設計不複雜、製造成本低廉下, 即達到分別保全不同使用者的專屬資訊。

以下將詳述應用根據本發明之第一較佳具體實施例之資訊保全裝置 10 的資訊處理流程。該資訊處理流程係執行於該通訊設備 1 內, 用以保全該通訊設備 1 之一用戶的資訊。該通訊設備 1 並且包含一密鑰產生模組 12, 該密鑰產生模組 12 係用以產生一密鑰。

請參考圖二所示, 首先, 執行步驟 S20, 傳送一輸入資料至該密鑰產生模組 12。接著, 執行步驟 S21, 接收由該密鑰產生模組 12 回應該輸入資料所產生之一密鑰。隨後, 執行步驟 S22, 使用該密鑰對該用戶之資訊加密, 進而產生一加密資訊。



五、發明說明 (8)

接著，執行步驟 S23，判斷該用戶之資訊是否需要被使用。若步驟 S23之結果為肯定，亦即經加密之該用戶的資訊要求被解密，以被使用時，則執行步驟 S24。

於步驟 S24中，再次傳送該輸入資料至該密鑰產生模組 12。於步驟 S24之後，接著執行步驟 S25。於步驟 S25中，接收由該密鑰產生模組 12回應該輸入資料再次產生之密鑰。於步驟 S25之後，接著執行步驟 S26。於步驟 S26中，使用該密鑰對加密資訊解密，進而恢復該用戶之資訊。

為加強保全通訊設備之用戶的資訊，於本發明之第二較佳具體實施例中，關於密鑰取得模組傳送至密鑰產生模組之輸入資料係為一隨機資料。以下將對本發明之第二較佳具體實施例之架構及運作原理，做一充分解說。

請參考圖三，圖三係為根據本發明之第二較佳具體實施例之資訊保全裝置 30的架構之示意圖。該資訊保全裝置 30係用於一通訊設備 3內，用以保全該通訊設備 3之一用戶的資訊。該通訊設備 3並且包含一密鑰產生模組 32，該密鑰產生模組 32係用以產生一密鑰。

該資訊保全裝置 30包含一儲存模組 302、一隨機資料產生模組 302、一密鑰取得模組 304、一加密模組 306，以及一解密模組 308。關於該儲存模組 302，該用戶之資訊係儲存於該儲存模組 302內。該隨機資料產生模組 303係用以產生一隨機輸入資料。該密鑰取得模組 304係用以從該隨機資料產生模組 303處接收該隨機輸入資料，並且傳送該



五、發明說明 (9)

隨機輸入資料至該密鑰產生模組 32。該密鑰產生模組 32 於接收到該隨機輸入資料後。會回應該隨機輸入資料，並且產生一密鑰。隨後，該密鑰取得模組 304 接收由該密鑰產生模組 32 回應該隨機輸入資料所產生之密鑰。

於一具體實施例中，該密鑰產生模組 32 係具有一預定演算邏輯，例如，圖三中所示的預定演算邏輯 322。該隨機輸入資料係被代入該演算邏輯 322 中，經過演算進而產生該密鑰。

於一具體實施例中，該密鑰產生模組 32 係為一用戶資訊模組卡 (SIM card)。該預定演算邏輯係可為一 HMAC 演算邏輯、一 GSM-A3 演算邏輯或一 GSM-A8 演算邏輯...等。

該加密模組 306 係用以經由該密鑰取得模組 304 擷取該密鑰，並且從該儲存模組 302 擷取該用戶之資訊。隨後，該加密模組 306 使用該密鑰對該用戶之資訊加密，進而產生一加密資訊。需說明的是，於產生該加密資訊之後，該加密資訊係併著該隨機輸入資料儲存於該儲存模組 302 內，並且置換儲存於該儲存模組 302 內之用戶之資訊。於實際應用中，如圖三所示，該加密模組 306 係由來自該通訊設備 3 之一驅動訊號所驅動，進而對該用戶之資訊加密。

進一步，當該用戶之資訊需要被使用時，該解密模組 306 係用以經由該密鑰取得模組 304 擷取該密鑰，並且從該儲存模組 302 擷取該加密資訊。隨後，該解密模組 308 使用該密鑰對該加密資訊解密，進而恢復該用戶之資訊。需說



五、發明說明 (10)

明的是，當該解密模組 308 經由該密鑰取得模組 304 擷取該密鑰時，該密鑰取得模組 304 則從該儲存模組 302 擷取該隨機輸入資料，再次傳送該隨機輸入資料至該密鑰產生模組 32，並且隨後接收由該密鑰產生模組 32 回應該隨機輸入資料而再次產生之密鑰。於實際應用中，如圖三所示，該解密模組 308 係由來自該通訊設備 3 之一驅動訊號所驅動，進而對該加密資訊解密。

於實際應用中，該加密模組 306 以及該解密模組 308 係可以整合成一個模組。

由以上對第二較佳具體實施例的詳述，可清楚的瞭解藉由隨機資料產生模組產生隨機輸入資料，將可增強對用戶之資訊的保全。

以下將詳述應用根據本發明之第二較佳具體實施例之資訊保全裝置 30 的資訊處理流程。該資訊處理流程係執行於該通訊設備 3 內，用以保全該通訊設備 3 之一用戶的資訊。該通訊設備 3 並且包含一密鑰產生模組 32，該密鑰產生模組 32 係用以產生一密鑰。

請參考圖四所示，首先，執行步驟 S40，產生一隨機輸入資料。接著，執行步驟 S41，傳送該隨機輸入資料至該密鑰產生模組 32。接著，執行步驟 S42，接收由該密鑰產生模組 32 回應該隨機輸入資料所產生之一密鑰。隨後，執行步驟 S43，使用該密鑰對該用戶之資訊加密，進而產生一加密資訊。

接著，執行步驟 S44，判斷該用戶之資訊是否需要被

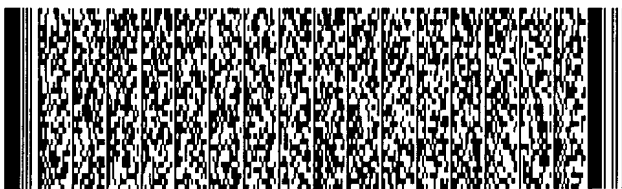


五、發明說明 (11)

使用。若步驟 S44之結果為肯定，亦即經加密之該用戶的資訊要求被解密，以被使用時，則執行步驟 S45。

於步驟 S45中，再次傳送該隨機輸入資料至該密鑰產生模組 32。於步驟 S45之後，接著執行步驟 S46。於步驟 S46中，接收由該密鑰產生模組 32回應該隨機輸入資料再次產生之密鑰。於步驟 S46之後，接著執行步驟 S47。於步驟 S47中，使用該密鑰對加密資訊解密，進而恢復該用戶之資訊。

藉由以上較佳具體實施例之詳述，係希望能更加清楚描述本發明之特徵與精神，而並非以上述所揭露的較佳具體實施例來對本發明之範疇加以限制。相反地，其目的是希望能涵蓋各種改變及具相等性的安排於本發明所欲申請之專利範圍的範疇內。



圖式簡單說明

圖式之簡易說明

圖一係為根據本發明之第一較佳具體實施例之一用於通訊設備內之資訊保全裝置的架構之示意圖，以及資訊保全裝置與通訊設備之間關係的示意圖。

圖二係繪出應用根據本發明之第一較佳具體實施例之資訊保全裝置的資訊處理流程。

圖三係為根據本發明之第二較佳具體實施例之一用於通訊設備內之資訊保全裝置的架構之示意圖，以及資訊保全裝置與通訊設備之間關係的示意圖。

圖四係繪出應用根據本發明之第二較佳具體實施例之資訊保全裝置的資訊處理流程。

圖式之標號說明

| | |
|----------------|--------------|
| 1、3：通訊設備 | 10、30：資訊保全裝置 |
| 12、32：密鑰產生模組 | 102、302：儲存模組 |
| 104、304：密鑰取得模組 | 106、306：加密模組 |
| 108、308：解密模組 | |
| 303：隨機資料產生模組 | |
| 122、322：預定演算邏輯 | |



六、申請專利範圍

1、一種用於一通訊設備內之裝置，該裝置係用以保全一用戶 (Subscriber)之一資訊，該通訊設備包含一密鑰產生模組 (Cipher key generating module)，該裝置包含：

一儲存模組，係用以儲存該用戶之資訊；

一密鑰取得模組 (Cipher key acquiring module)，係用以傳送一輸入資料至該密鑰產生模組，並且隨後接收由該密鑰產生模組回應該輸入資料所產生之一密鑰 (Cipher key)；

一加密模組 (Encrypting module)，係用以經由該密鑰取得模組擷取該密鑰，並且從該儲存模組擷取該用戶之資訊，並且隨後使用該密鑰對該用戶之資訊加密，進而產生一加密資訊，其中，於產生該加密資訊之後，該加密資訊係儲存於該儲存模組內並且置換儲存於該儲存模組內該用戶之資訊；以及

一解密模組 (Decrypting module)，當該用戶之資訊需要被使用時，該解密模組係用以經由該密鑰取得模組擷取該密鑰，並且從該儲存模組擷取該加密資訊，並且隨後使用該密鑰對該加密資訊解密，進而恢復該用戶之資訊，其中，當該解密模組經由該密鑰取得模組擷取該密鑰時，該密鑰取得模組則再次傳送該輸入資料至該密鑰產生模組，並且隨後接收由該密鑰產生模組回應該輸入資料再次產生之該密鑰。

2、如申請專利範圍第 1 項所述之裝置，其中該輸入資料



六、申請專利範圍

係預存於該通訊設備之一硬體序號。

3、如申請專利範圍第1項所述之裝置，其中該密鑰產生模組內預先存有一使用者代號，該密鑰產生模組係回應該輸入資料進而輸出該使用者代號做為該密鑰之用。

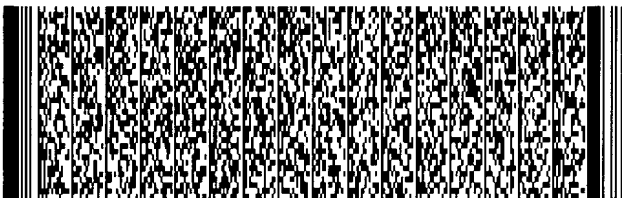
4、如申請專利範圍第1項所述之裝置，其中該密鑰產生模組係為一用戶資訊模組卡 (Subscriber Information Module card, SIM card)。

5、如申請專利範圍第1項所述之裝置，其中該加密模組與該解密模組係整合為同一模組。

6、如申請專利範圍第1項所述之裝置，其中該密鑰產生模組係具有一預定演算邏輯，並且該輸入資料係被代入該演算邏輯，進而產生該密鑰。

7、如申請專利範圍第6項所述之裝置，其中該預訂演算邏輯係為從由一 HMAC (Hash-based Message Authentication Code) 演算邏輯、一 GSM-A3 演算邏輯以及一 GSM-A8 演算邏輯所組成之一群組當中所選取之一演算邏輯。

8、一種用於一通訊設備內之裝置，該裝置係用以保全一



六、申請專利範圍

用戶 (Subscriber) 之一資訊，該通訊設備包含一密鑰產生模組 (Cipher key generating module)，該裝置包含：

- 一儲存模組，係用以儲存該用戶之資訊；
- 一隨機資料產生模組，係用以產生一隨機輸入資料；
- 一密鑰取得模組 (Cipher key acquiring module)，

係用以從該隨機資料產生模組接收該隨機輸入資料，並且傳送該隨機輸入資料至該密鑰產生模組，並且隨後接收由該密鑰產生模組回應該隨機輸入資料所產生之一密鑰 (Cipher key)；

一加密模組 (Encrypting module)，係用以經由該密鑰取得模組擷取該密鑰，並且從該儲存模組擷取該用戶之資訊，並且隨後使用該密鑰對該用戶之資訊加密，進而產生一加密資訊，其中，於產生該加密資訊之後，該加密資訊係併著該隨機輸入資料儲存於該儲存模組內，並且該加密資訊係置換儲存於該儲存模組內的該用戶之資訊；以及

一解密模組 (Decrypting module)，當該用戶之資訊需要被使用時，該解密模組係用以經由該密鑰取得模組擷取該密鑰，並且從該儲存模組擷取該加密資訊，並且隨後使用該密鑰對該加密資訊解密，進而恢復該用戶之資訊，其中，當該解密模組經由該密鑰取得模組擷取該密鑰時，該密鑰取得模組則從該儲存模組擷取該隨機輸入資料，再次傳送該隨機輸入資料至該密鑰產生模組，並且隨後接收由該密鑰產生模組回應該隨機輸入資料再次產生之該密鑰。



六、申請專利範圍

9、如申請專利範圍第8項所述之裝置，其中該密鑰產生模組係具有一預定演算邏輯，並且該輸入資料係被代入該演算邏輯，進而產生該密鑰。

10、如申請專利範圍第9項所述之裝置，其中該密鑰產生模組係為一用戶資訊模組卡 (Subscriber Information Module card, SIM card)。

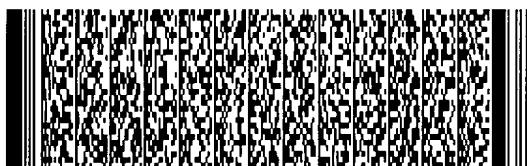
11、如申請專利範圍第10項所述之裝置，其中該預訂演算邏輯係為從由一 HMAC (Hash-based Message Authentication Code) 演算邏輯、一 GSM-A3 演算邏輯以及一 GSM-A8 演算邏輯所組成之一群組當中所選取之一演算邏輯。

12、如申請專利範圍第11項所述之裝置，其中該加密模組與該解密模組係整合為同一模組。

13、一種執行於一通訊設備內之資訊處理方法，該資訊處理方法係用以保全一用戶 (Subscriber) 之一資訊，該通訊設備包含一密鑰產生模組 (Cipher key generating module)，該資訊處理方法包含下列步驟：

傳送一輸入資料至該密鑰產生模組；

接收由該密鑰產生模組回應該輸入資料所產生之一密



六、申請專利範圍

鑰 (Cipher key);

使用該密鑰對該用戶之資訊加密，進而產生一加密資訊；以及

當該用戶之資訊需要被使用時，再次傳送該輸入資料至該密鑰產生模組，接收由該密鑰產生模組回應該輸入資料再次產生之該密鑰，並且使用該密鑰對該加密資訊解密，進而恢復該用戶之資訊。

14、如申請專利範圍第13項所述之資訊處理方法，其中該輸入資料係預存於該通訊設備內之一硬體序號。

15、如申請專利範圍第13項所述之資訊處理方法，其中該密鑰產生模組係具有一預定演算邏輯，並且該輸入資料係被代入該演算邏輯，進而產生該密鑰。

16、如申請專利範圍第13項所述之資訊處理方法，其中該密鑰產生模組內預先存有一使用者代號，該密鑰產生模組係回應該輸入資料進而輸出該使用者代號做為該密鑰之用。

17、如申請專利範圍第13項所述之資訊處理方法，其中該密鑰產生模組係為一用戶資訊模組卡 (Subscriber Information Module card, SIM card)。



六、申請專利範圍

18、如申請專利範圍第 17 項所述之資訊處理方法，其中該預訂演算邏輯係為從由一 HMAC(Hash-based Message Authentication Code)演算邏輯、一 GSM-A3 演算邏輯以及一 GSM-A8 演算邏輯所組成之一群組當中所選取之一演算邏輯。

19、一種執行於一通訊設備內之資訊處理方法，該資訊處理方法係用以保全一用戶 (Subscriber) 之一資訊，該通訊設備包含一密鑰產生模組 (Cipher key generating module)，該資訊處理方法包含下列步驟：

產生一隨機輸入資料；

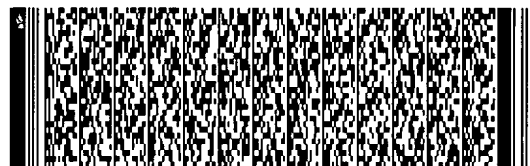
傳送該隨機輸入資料至該密鑰產生模組；

接收由該密鑰產生模組回應該隨機輸入資料所產生之一密鑰 (Cipher key)；

使用該密鑰對該用戶之資訊加密，進而產生一加密資訊；以及

當該用戶之資訊需要被使用時，再次傳送該隨機輸入資料至該密鑰產生模組，接收由該密鑰產生模組回應該隨機輸入資料再次產生之該密鑰，並且使用該密鑰對該加密資訊解密，進而恢復該用戶之資訊。

20、如申請專利範圍第 19 項所述之資訊處理方法，其中該密鑰產生模組係具有一預定演算邏輯，並且該輸入資料係被代入該演算邏輯，進而產生該密鑰。



六、申請專利範圍

21、如申請專利範圍第 20 項所述之資訊處理方法，其中該密鑰產生模組係為一用戶資訊模組卡 (Subscriber Information Module card, SIM card)。

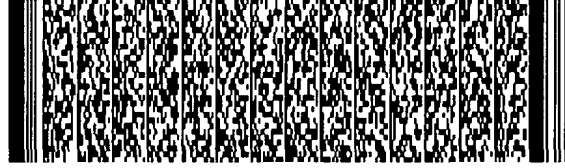
22、如申請專利範圍第 21 項所述之資訊處理方法，其中該預訂演算邏輯係為從由一 HMAC (Hash-based Message Authentication Code) 演算邏輯、一 GSM-A3 演算邏輯以及一 GSM-A8 演算邏輯所組成之一群組當中所選取之一演算邏輯。



第 1/25 頁



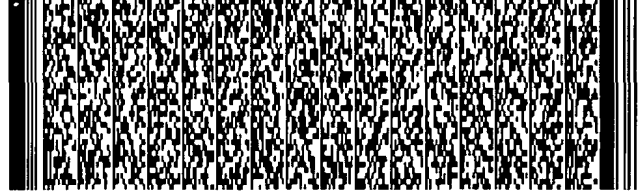
第 2/25 頁



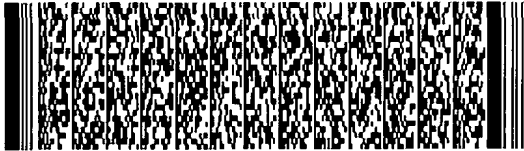
第 2/25 頁



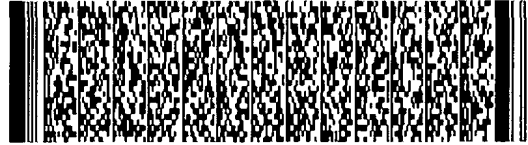
第 3/25 頁



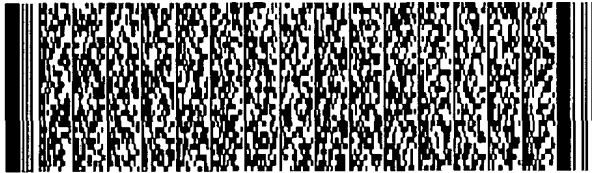
第 4/25 頁



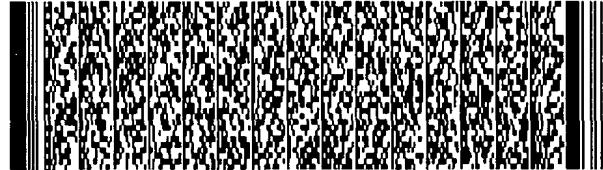
第 5/25 頁



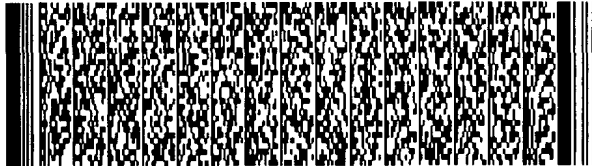
第 7/25 頁



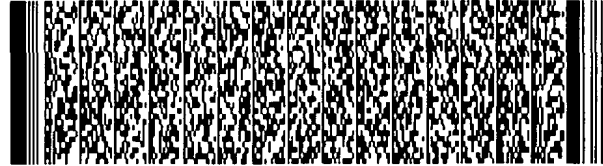
第 7/25 頁



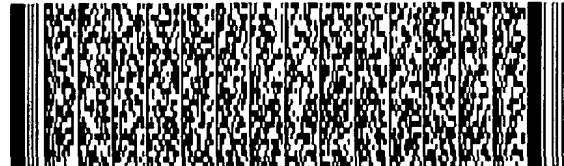
第 8/25 頁



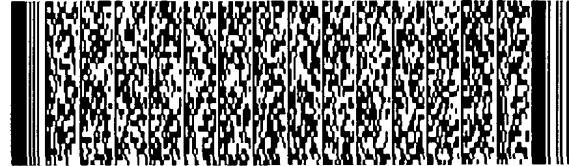
第 8/25 頁



第 9/25 頁



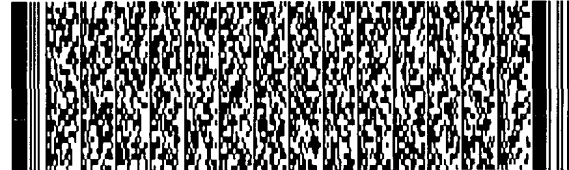
第 9/25 頁



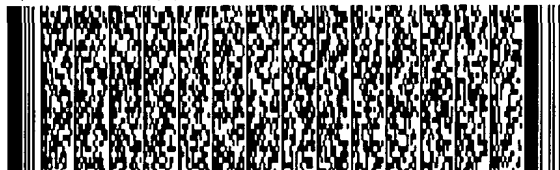
第 10/25 頁



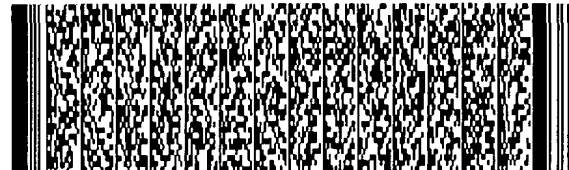
第 10/25 頁



第 11/25 頁



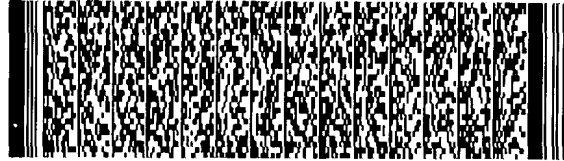
第 11/25 頁



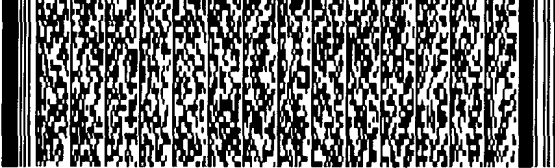
第 12/25 頁



第 12/25 頁



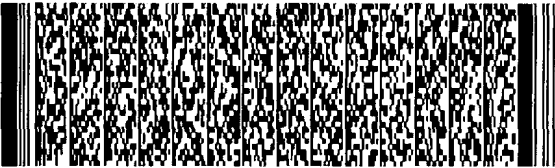
第 13/25 頁



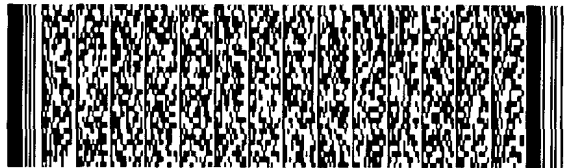
第 13/25 頁



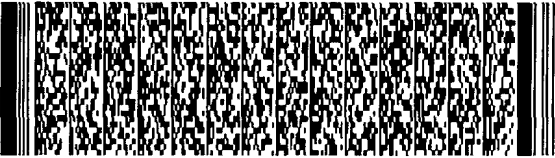
第 14/25 頁



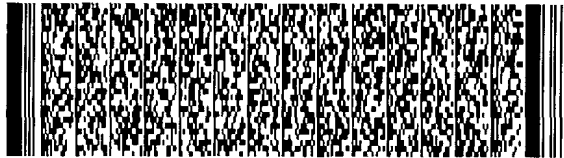
第 14/25 頁



第 15/25 頁



第 15/25 頁



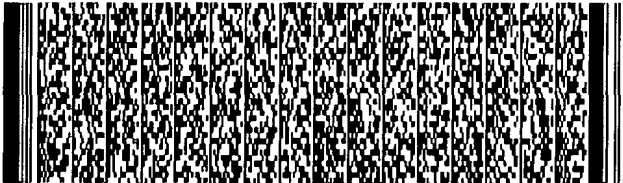
第 16/25 頁



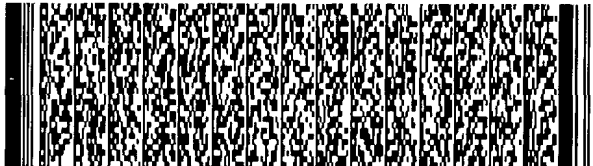
第 16/25 頁



第 17/25 頁



第 18/25 頁



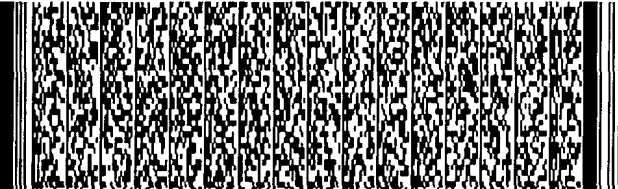
第 19/25 頁



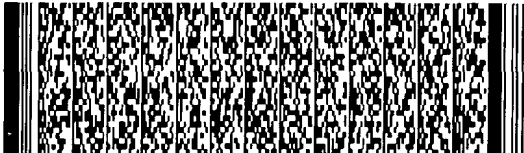
第 19/25 頁



第 20/25 頁



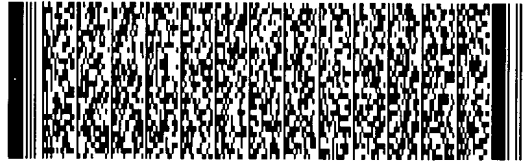
第 21/25 頁



第 21/25 頁



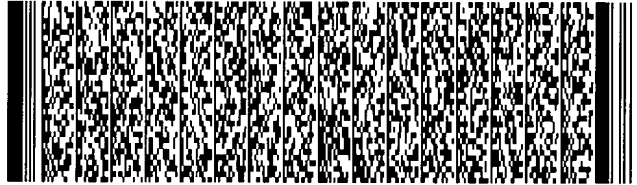
第 22/25 頁



第 22/25 頁



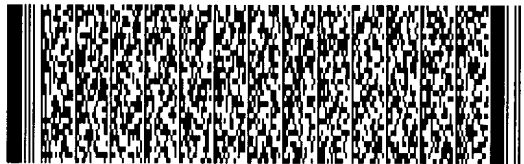
第 23/25 頁



第 24/25 頁

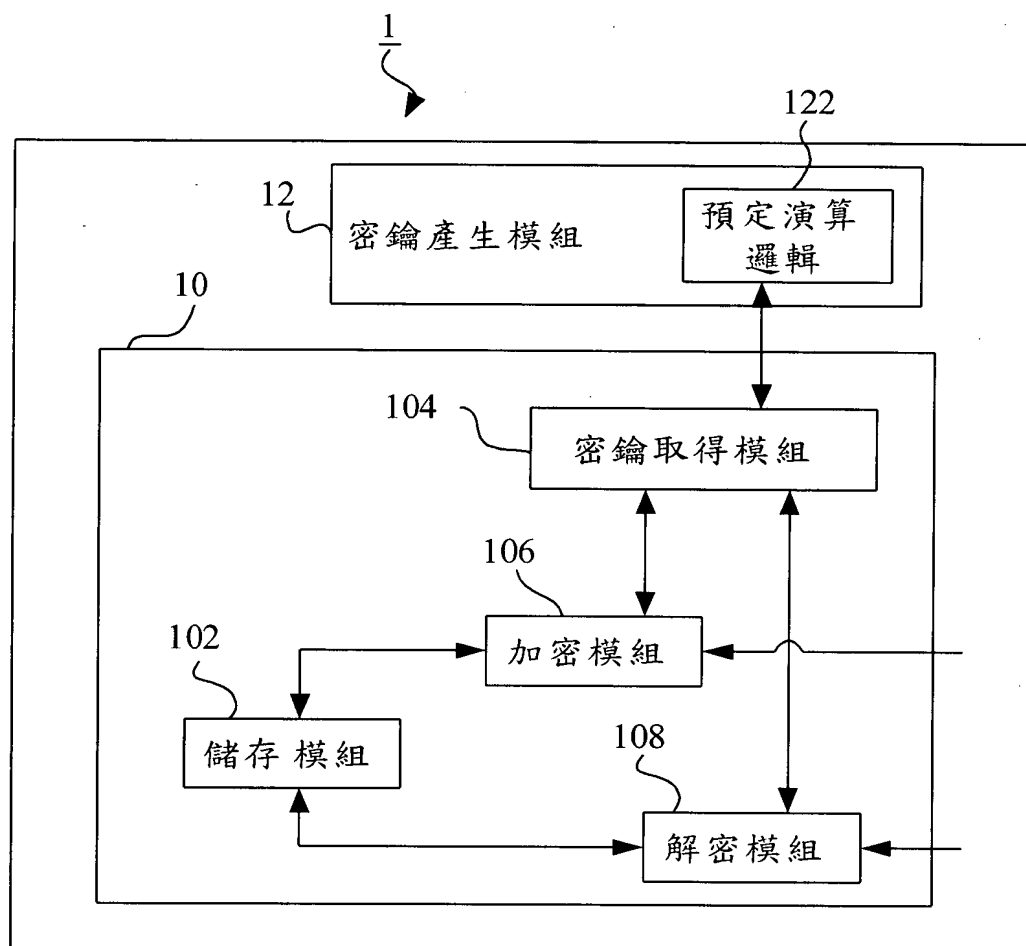


第 24/25 頁

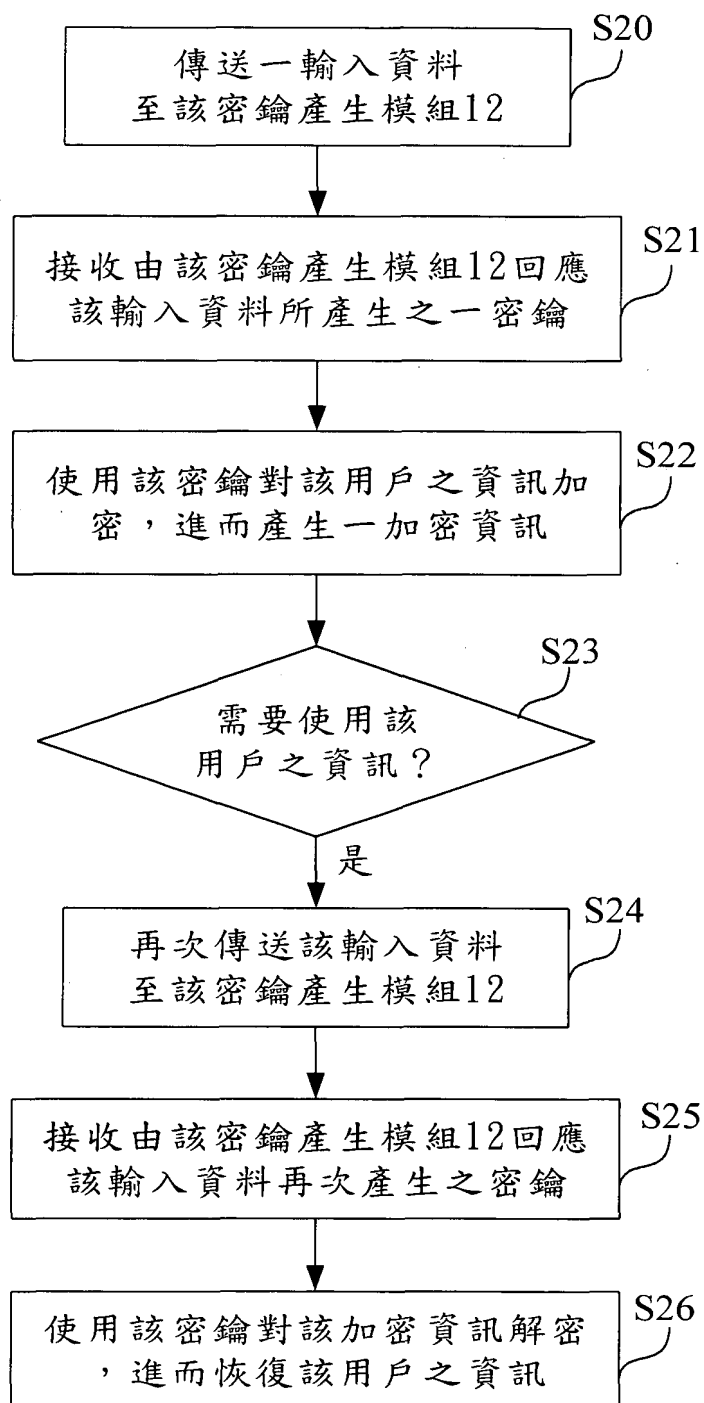


第 25/25 頁





圖一



圖二

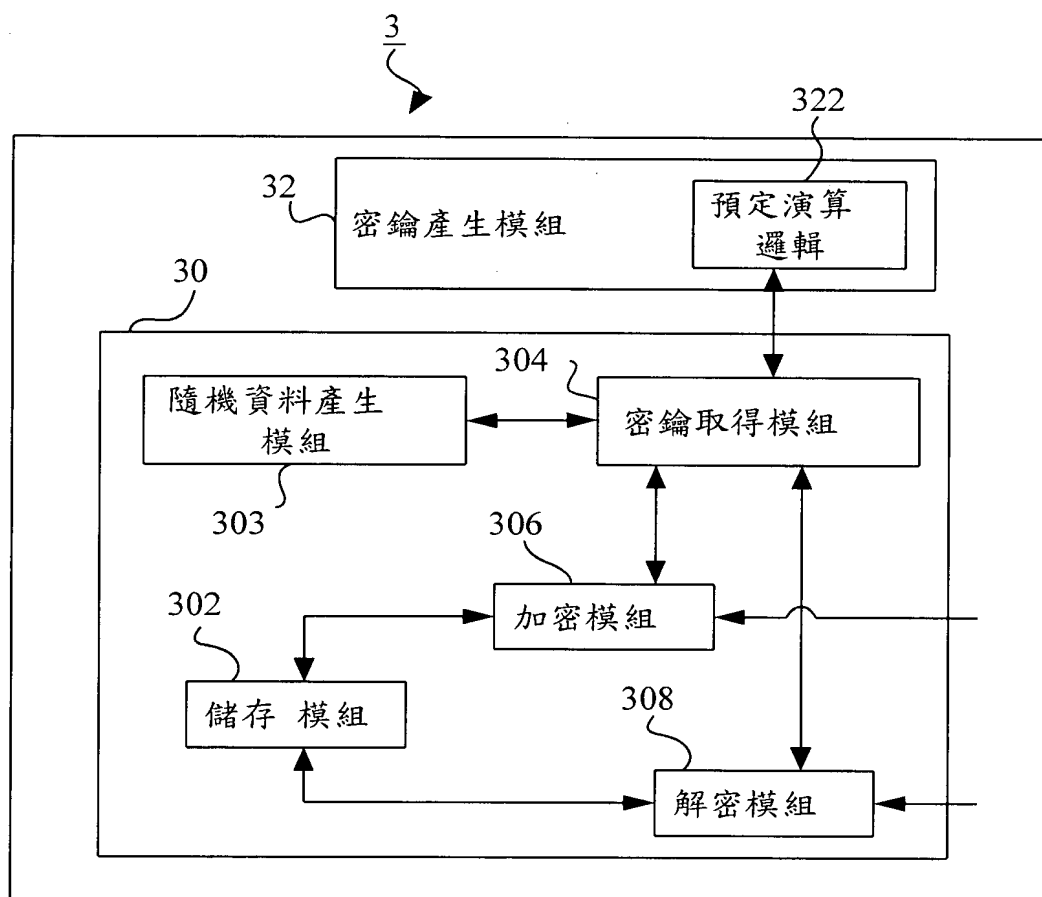
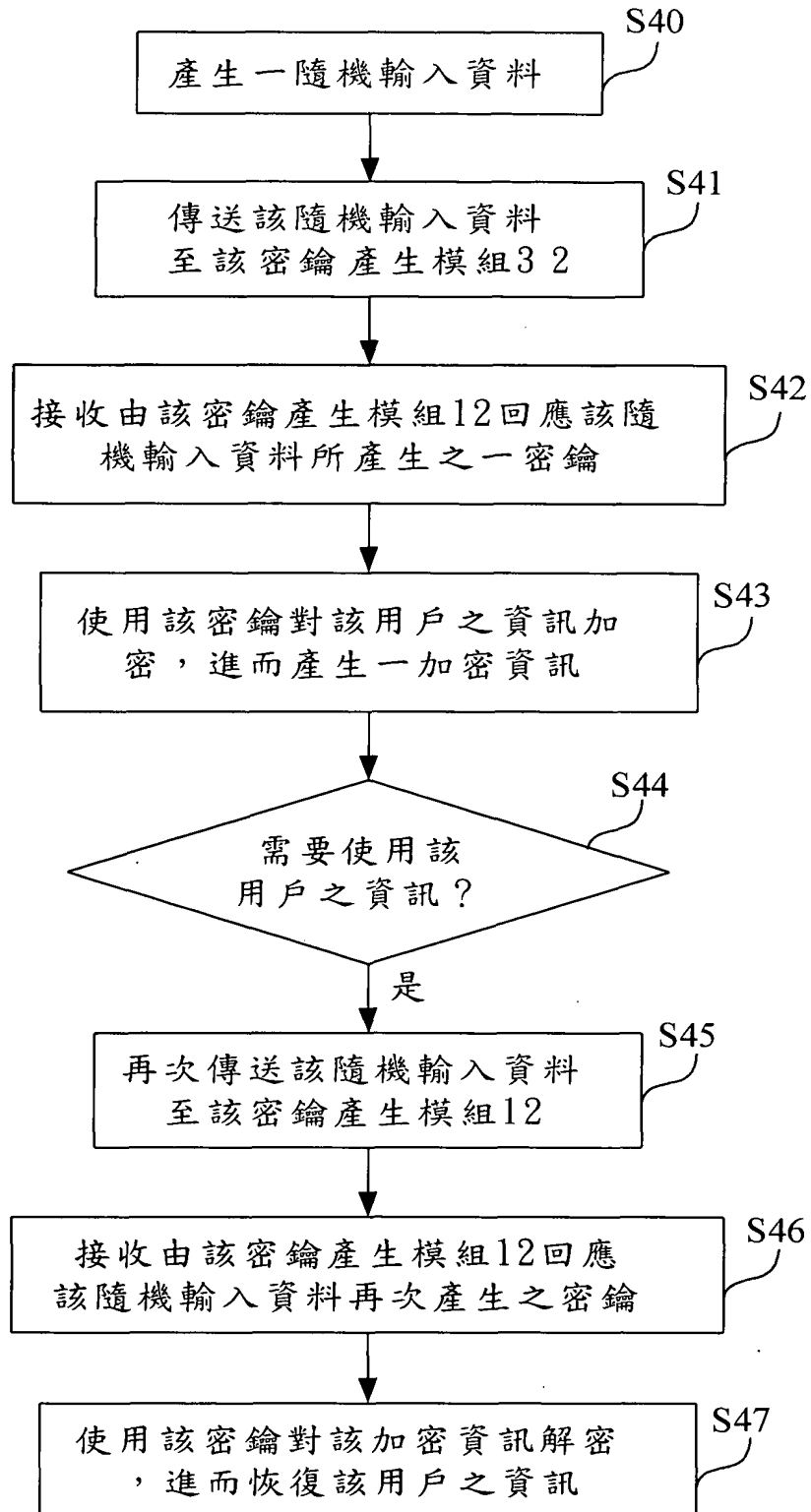


圖 三



圖四